IN THE CLAIMS

Please cancel claims 4, 8-9, 18, 42-43, 55-56 and 66-67.

Please amend the claims as follows.

1. (Currently Amended) An apparatus comprising:

at least one processor;

a memory coupled to the at least one processor;

a first program residing in the memory;

a second program residing in the memory;

a third program residing in the memory;

a dynamic key generation mechanism that dynamically generates public/private key pairs; and

an inter-program authentication mechanism that authenticates the first program to the second program ~~using a public/private key pair that is dynamically generated by the dynamic key generation mechanism~~ using a first authentication token that is digitally signed by the first program using a private key that is dynamically generated by the dynamic key generation mechanism, that authenticates the second program to the first program, if required, by digitally signing the first authentication token using a private key corresponding to the second program to generate therefrom a second authentication token, and returning the second authentication token to the first program, and that authenticates the second program to the third program by generating a third authentication token from the first authentication token received from the first program, and sending the third authentication token to the third program.

2. (Original) The apparatus of claim 1 wherein the first program includes an authentication mechanism that authenticates a user.

3. (Original) The apparatus of claim 1 wherein, after the inter-program authentication mechanism authenticates the first program to the second program, the second program performs identity mapping from an identity asserted by the first program to an identity understood by the second program.

4 (Cancelled)

5. (Currently Amended) The apparatus of claim [[4]] 1 wherein the first authentication token comprises:

information about a user that authenticates with the first program;

information about the first program;

information about the second program; and

a digital signature of the first program using a private key for the first program generated by the dynamic key generation mechanism.

6. (Currently Amended) The apparatus of claim [[4]] 1 wherein the second program verifies the first authentication token by querying a public key authority for the public key corresponding to the first program.

7. (Original) The apparatus of claim 6 wherein the second program verifies the first authentication token by verifying the digital signature of the first program using the public key for the first program retrieved from the public key authority.

8-9 (Cancelled)

10. (Currently Amended) The apparatus of claim [[9]] 1 wherein the third program verifies the third authentication token by querying a public key authority for the public key corresponding to the second program.

11. (Original) The apparatus of claim 1 further comprising log file that is written to each time a program verifies an authentication token.

12. (Currently Amended) An apparatus comprising:

at least one processor;

a memory coupled to the at least one processor;

a first program residing in the memory, the first program including an authentication mechanism that authenticates a user;

a second program residing in the memory;

a dynamic key generation mechanism that dynamically generates public/private key pairs;

a public key authority that publishes public keys generated by the dynamic key generation mechanism; and

an inter-program authentication mechanism that authenticates the first program to the second program using a first authentication token that is digitally signed by the first program using a private key that is dynamically generated by the dynamic key generation mechanism and that authenticates the second program to the first program, if required, by digitally signing the first authentication token using a private key corresponding to the second program to generate therefrom a second authentication token, and returning the second authentication token to the first program.

13. (Original) The apparatus of claim 12 wherein, after the inter-program authentication mechanism authenticates the first program to the second program, the second program performs identity mapping from an identity asserted by the first program to an identity understood by the second program.

14. (Original) The apparatus of claim 12 wherein the first authentication token comprises:

information about a user that authenticates with the first program;

information about the first program;

information about the second program; and

a digital signature of the first program using a private key for the first program generated by the dynamic key generation mechanism.

15. (Original) The apparatus of claim 12 wherein the second program verifies the first authentication token by querying the public key authority for the public key corresponding to the first program.

16. (Original) The apparatus of claim 15 wherein the second program verifies the first authentication token by verifying the digital signature of the first program using the public key for the first program retrieved from the public key authority.

17. (Original) The apparatus of claim 12 wherein the second program authenticates to the first program, if required, by digitally signing the first authentication token using a private key corresponding to the second program to generate therefrom a second authentication token, and returning the second authentication token to the first program.

18. (Cancelled)

19. (Currently Amended) The apparatus of claim [[18]] 12 wherein the third program verifies the third authentication token by querying the public key authority for the public key corresponding to the second program.

20. (Original) The apparatus of claim 12 further comprising a log file that is written to each time a program verifies an authentication token.

21. (Original) An apparatus comprising:

at least one processor;

a memory coupled to the at least one processor;

a first program residing in the memory;

a second program residing in the memory;

a third program residing in the memory;

a dynamic key generation mechanism that dynamically generates public/private key pairs; and

an inter-program authentication mechanism that authenticates the first program to the second program using a first authentication token generated by the first program using a public/private key pair corresponding to the first program, and that authenticates the second program to the third program using a second authentication token that includes all information in the first authentication token.

22. (Original) A method for a first program to authenticate to a second program, the method comprising the steps of:

(A) dynamically generating a public/private key pair for the first program;

(B) the first program generating a first authentication token using the private key dynamically generated in step (A); and

(C) the second program verifying the first authentication token using the public key dynamically generated in step (A).

23. (Original) The method of claim 22 wherein the second program verifies the first authentication token in step (C) by verifying a digital signature of the first program in the authentication token using the public key for the first program.

24. (Original) The method of claim 22 further comprising the step of authenticating a user to the first program.

25. (Original) The method of claim 22 further comprising the step of performing identity mapping from an identity asserted by the first program to an identity understood by the second program.

26. (Original) The method of claim 22 wherein the first authentication token comprises:

information about a user that authenticates with the first program;

information about the first program;

information about the second program; and

a digital signature of the first program using a private key for the first program generated by the dynamic key generation mechanism.

27. (Original) The method of claim 22 further comprising the steps of:

(D) dynamically generating a public/private key pair for the second program;

(E) the second program digitally signing the first authentication token using the private key generated in step (D) to generate therefrom a second authentication token; and

(F) returning the second authentication token to the first program to authenticate the second program to the first program.

28. (Original) The method of claim 22 further comprising the step of the second program authenticating to a third program by generating a third authentication token from the first authentication token and sending the third authentication token to the third program.

29. (Original) The method of claim 28 further comprising the step of the third program verifying the third authentication token by using the public key generated in step (D).

30. (Original) The method of claim 22 further comprising the step of writing to a log file that is written to each time a program verifies an authentication token.

31. (Original) A method for a first program to authenticate to a second program, the method comprising the steps of:

(A) dynamically generating a public/private key pair for the first program;

(B) sending the public key for the first program to a public key authority;

(C) dynamically generating a public/private key pair for the second program;

(D) sending the public key for the second program to the public key authority;

(E) the first program generating a first authentication token using the private key for the first program; and

(F) the second program verifying the first authentication token by querying the public key authority for the public key corresponding to the first program.

32. (Original) The method of claim 31 wherein the second program verifies the first authentication token in step (F) by verifying a digital signature of the first program in the authentication token using the public key for the first program retrieved from the public key authority.

33. (Original) The method of claim 31 further comprising the step of authenticating a user to the first program.

34. (Original) The method of claim 31 further comprising the step of performing identity mapping from an identity asserted by the first program to an identity understood by the second program.

35. (Original) The method of claim 31 wherein the first authentication token comprises:

information about a user that authenticates with the first program;

information about the first program;

information about the second program; and

a digital signature of the first program using a private key for the first program generated by the dynamic key generation mechanism.

36. (Original) The method of claim 31 further comprising the steps of:

(G) dynamically generating a public/private key pair for the second program;

(H) the second program digitally signing the first authentication token using the private key generated in step (G) to generate therefrom a second authentication token; and

(I) returning the second authentication token to the first program to authenticate the second program to the first program.

37. (Original) The method of claim 31 further comprising the step of the second program authenticating to a third program by generating a third authentication token from the first authentication token and sending the third authentication token to the third program.

38. (Original) The method of claim 37 further comprising the step of the third program verifying the third authentication token by using the public key corresponding to the second program.

39. (Original) The method of claim 31 further comprising the step of writing to a log file that is written to each time a program verifies an authentication token.

40. (Original) A method for authenticating a first program to a third program, the method comprising the steps of:

authenticating the first program to a second program using a first authentication token generated by the first program using a public/private key pair corresponding to the first program; and

authenticating the second program to the third program using a second authentication token that includes all information in the first authentication token.

41. (Currently Amended) A computer-readable program product comprising:

(A) an inter-program authentication mechanism that authenticates a first program to a second program using a public/private key pair that is dynamically generated by a dynamic key generation mechanism; and

(B) ~~computer-readable signal bearing~~ recordable media bearing the inter-program authentication mechanism.

42-43 (Cancelled)

44. (Original) The program product of claim 41 wherein the first program includes an authentication mechanism that authenticates a user.

45. (Original) The program product of claim 41 wherein, after the inter-program authentication mechanism authenticates the first program to the second program, the second program performs identity mapping from an identity asserted by the first program to an identity understood by the second program.

46. (Original) The program product of claim 41 wherein the first program authenticates to the second program using a first authentication token that is digitally signed by the first program using a key that is dynamically generated by the dynamic key generation mechanism.

47. (Original) The program product of claim 46 wherein the first authentication token comprises:

information about a user that authenticates with the first program;

information about the first program;

information about the second program; and

a digital signature of the first program using a private key for the first program generated by the dynamic key generation mechanism.

48. (Original) The program product of claim 46 wherein the second program verifies the first authentication token by querying the public key authority for the public key corresponding to the first program.

49. (Original) The program product of claim 48 wherein the second program verifies the first authentication token by verifying the digital signature of the first program using the public key for the first program retrieved from the public key authority.

50. (Original) The program product of claim 46 wherein the second program authenticates to the first program, if required, by digitally signing the first authentication token using a private key corresponding to the second program to generate therefrom a second authentication token, and returning the second authentication token to the first program.

51. (Original) The program product of claim 50 further comprising a third program, wherein the second program authenticates to the third program by generating a third authentication token from the first authentication token received from the first program, and sending the third authentication token to the third program.

52. (Original) The program product of claim 51 wherein the third program verifies the third authentication token by querying the public key authority for the public key corresponding to the second program.

53. (Original) The program product of claim 41 further comprising log file that is written to each time a program verifies an authentication token.

54. (Currently Amended) A computer-readable program product comprising:

(A) an inter-program authentication mechanism that authenticates a first program to a second program using a first authentication token that is digitally signed by the first program using a key that is dynamically generated by a dynamic key generation mechanism in a public key authority, the first program including an authentication mechanism that authenticates a user; and

(B) ~~computer-readable signal bearing~~ recordable media bearing the inter-program authentication mechanism.

55-56 (Cancelled)

57. (Original) The program product of claim 54 wherein, after the inter-program authentication mechanism authenticates the first program to the second program, the second program performs identity mapping from an identity asserted by the first program to an identity understood by the second program.

58. (Original) The program product of claim 54 wherein the first authentication token comprises:

information about a user that authenticates with the first program;

information about the first program;

information about the second program; and

a digital signature of the first program using a private key for the first program generated by the dynamic key generation mechanism.

59. (Original) The program product of claim 54 wherein the second program verifies the first authentication token by querying the public key authority for the public key corresponding to the first program.

60. (Original) The program product of claim 59 wherein the second program verifies the first authentication token by verifying the digital signature of the first program using the public key for the first program retrieved from the public key authority.

61. (Original) The program product of claim 54 wherein the second program authenticates to the first program, if required, by digitally signing the first authentication token using a private key corresponding to the second program to generate therefrom a second authentication token, and returning the second authentication token to the first program.

62. (Original) The program product of claim 61 further comprising a third program, wherein the second program authenticates to the third program by generating a third authentication token from the first authentication token received from the first program, and sending the third authentication token to the third program.

63. (Original) The program product of claim 61 wherein the third program verifies the third authentication token by querying the public key authority for the public key corresponding to the second program.

64. (Original) The program product of claim 54 further comprising a log file that is written to each time a program verifies an authentication token.

65. (Currently Amended) A computer-readable program product comprising:

(A) an inter-program authentication mechanism that authenticates a first program to a second program using a first authentication token generated by the first program using a public/private key pair corresponding to the first program, and that authenticates the second program to a third program using a second authentication token that includes all information in the first authentication token; and

(B) ~~computer-readable signal bearing~~ recordable media bearing the inter-program authentication mechanism.

66-67. (Cancelled)